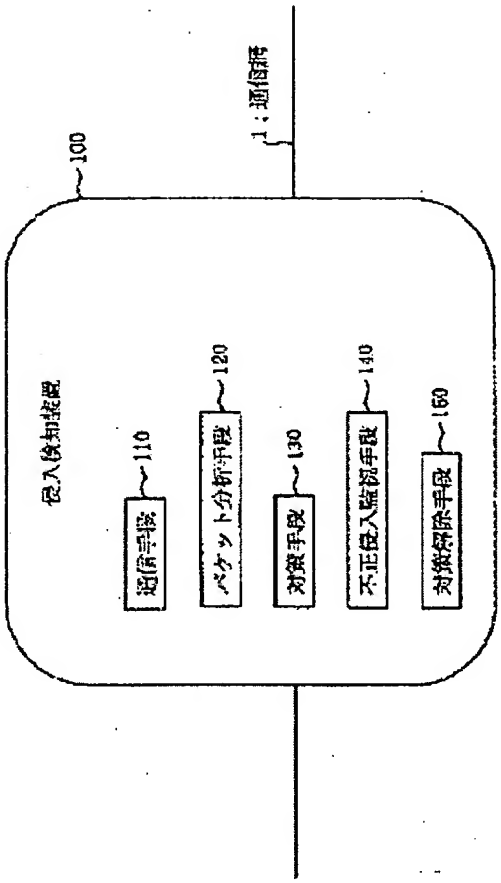
BREAK-IN DETECTING DEVICE AND ILLEGAL BREAK-IN MEASURES MANAGEMENT SYSTEM AND BREAK-IN DETECTING METHOD

Patent number: JP2002073433
Publication date: 2002-03-12
Inventor: OGOSHI TAKEHIRO
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
- international: G06F13/00; H04L12/24; H04L12/26; H04L12/66; H04L12/56; H04L12/22
- european:
Application number: JP20000256571 20000828
Priority number(s):

Abstract of **JP2002073433**

PROBLEM TO BE SOLVED: To provide a break-in detecting device which detects illegal break-in by judging from packets, and if illegal break-in occurs, takes measures to prevent illegal break-in.

SOLUTION: In a computer network system, the break-in detecting device 100 is provided with the following: a communication means 110; a packet analyzing means 120 that determines whether or not the illegal break-in is proceeding by analyzing the received packets; a measure means 130 that if it is judged that the illegal break-in is proceeding, performs closing of protocol processing or ports, shutting down of communication and the like; an illegal break-in monitoring means 140 that monitors whether or not the attack of illegal break-in and the like is terminated; and a measure removing means 150 that if it is judged that the attack of illegal break-in and the like is terminated, removes the measures of shutting down of communication and the like.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－73433
（P2002－73433A）
(43)公開日　平成14年３月12日(2002.3.12)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
G06F 13/00	351	G06F 13/00	351Z 5B089
H04L 12/24		H04L 11/08	5K030
12/26		11/20	B
12/66			102A
12/56		11/26	

審査請求　未請求　請求項の数11　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願2000－256571(P2000－256571)

(22)出願日　平成12年８月28日(2000.8.28)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

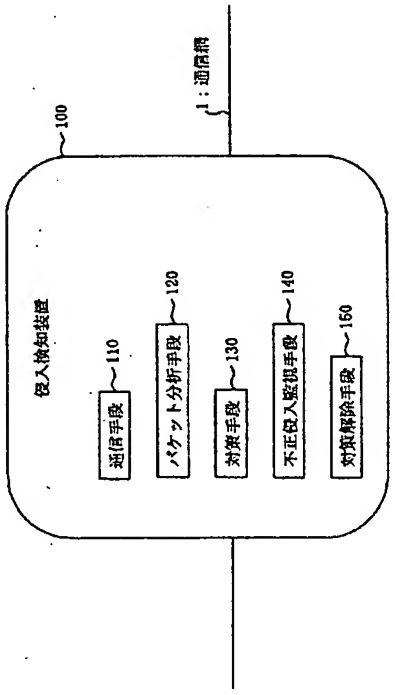
(72)発明者　大越　丈弘
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B089 GA31 GA33 GB02 KA17 KB02
KB13 KC28 KC47 KC52 KG05
KG06 MC02
5K030 GA15 HA08 JA03 JA10 JL08
KA04 KA13 LA01 LC13 MA04

(54)【発明の名称】　侵入検知装置及び不正侵入対策管理システム及び侵入検知方法

(57)【要約】
【課題】　不正侵入の検知をパケットから判断し、不正侵入があった場合、不正侵入を防止する対策をとる侵入検知装置を提供する。
【解決手段】　コンピュータネットワークシステムにおいて、侵入検知装置１００は、通信手段１１０と、受信したパケットを解析して不正侵入が行われているか否かを判断するパケット分析手段１２０と、不正侵入が行われていると判断した場合、プロトコル又はポートのクローズ、通信遮断等を行う対策手段１３０と、不正侵入等の攻撃が終了したか否かを監視する不正侵入監視手段１４０と、不正侵入等の攻撃が終了したと判断した場合、通信遮断等の対策を解除する対策解除手段１５０とを備える。



【特許請求の範囲】
【請求項1】 パケットを送受信する通信部と、
上記通信部が受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析部と、
上記パケット分析部が不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策部とを備えることを特徴とする侵入検知装置。
【請求項2】 上記侵入検知装置は、さらに、
上記パケット分析部の検出結果に基づいて上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視部と、
上記不正侵入監視部が、不正侵入終了を判断した場合、上記対策部がとる上記不正侵入を防止する対策を解除する対策解除部とを備えることを特徴とする請求項1記載の侵入検知装置。
【請求項3】 上記パケット分析部は、予め定義するデータを含むパケットを不正なパケットであるとすることを特徴とする請求項1または2記載の侵入検知装置。
【請求項4】 上記パケット分析部は、予め定義するデータとして、通信プロトコルの名称と通信ポートの番号と所定の文字列との少なくともいずれか一つを定義することを特徴とする請求項3記載の侵入検知装置。
【請求項5】 上記対策部は、不正侵入を防止する対策として、不正なパケットの通信を遮断することを特徴とする請求項1から4いずれかに記載の侵入検知装置。
【請求項6】 上記対策部は、通信の遮断として、使用していた通信ポートの使用を中止し、
上記侵入検知装置は、さらに、
上記対策部によって使用していた通信ポートの使用が中止されている場合、上記使用していた通信ポートとは別の通信ポートをオープンし、オープンした通信ポートを所定の送信元へ通知する通信ポート通知部を備えることを特徴とする請求項5記載の侵入検知装置。
【請求項7】 上記侵入検知装置は、さらに、
不正なパケットの受信が終了した場合に、使用を中止した通信ポートの使用を再開し、上記通信ポートの再開を上記所定の送信元へ通知する不正侵入終了通知部を備えることを特徴とする請求項6記載の侵入検知装置。
【請求項8】 情報処理装置と、上記情報処理装置と通信網を介して接続し、不正侵入を検知する侵入検知装置とを備える不正侵入対策管理システムにおいて、
上記侵入検知装置は、
上記通信網を介してパケットを送受信する通信部と、
上記受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析部と、
上記パケット分析部で不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策部と、
上記対策部によって使用していた通信ポートの使用が中止されている場合、上記使用していた通信ポートとは別の通信ポートをオープンし、オープンした通信ポートを上記情報処理装置へ通知する通信ポート通知部とを備え、
上記情報処理装置は、
上記通信網へパケットを送信すると伴に、上記通信ポート通知部から通知される通信ポートを受信する送受信部と、
上記送受信部によって受信した通信ポートを用いて通信することを設定するテンポラリポート設定部とを備えることを特徴とする不正侵入対策管理システム。
【請求項9】 上記侵入検知装置は、さらに、
上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視部と、
上記不正侵入監視部によって、不正侵入終了を判断した場合、上記不正侵入を防止する対策を解除する対策解除部と、
不正なパケットの受信が終了した場合に、使用を中止した通信ポートの使用を再開し、上記使用を中止した通信ポートの再開を上記情報処理装置へ通知する不正侵入終了通知部とを備え、
上記送受信部は、上記不正侵入終了通知部からの通知を受信し、
上記テンポラリポート設定部は、上記使用を中止した通信ポートを用いる通信へ設定を変更することを特徴とする請求項8記載の不正侵入対策管理システム。
【請求項10】 パケットを送受信する通信工程と、
上記受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析工程と、
上記パケット分析工程で不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策工程とを備えることを特徴とする侵入検知方法。
【請求項11】 上記侵入検知方法は、さらに、
上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視工程と、
上記不正侵入監視工程によって、不正侵入終了を判断した場合、上記不正侵入を防止する対策を解除する対策解除工程とを備えることを特徴とする請求項10記載の侵入検知方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】この発明は、コンピュータネットワークシステムに関するものである。
【0002】
【従来の技術】図7は、例えば、特開平11-177597に示された侵入防止機能付きハブに基づく従来の侵入防止機能付きハブの一例である。侵入防止機能付きハブは、パケットの送信元のアドレスから不正アクセスか

否か判断しようとするものである。図において、５０はハブである。５１はメモリである。５２はデータバスである。５３ｊ（ｊ＝１～Ｎ）はポート（ＰＨＹ：物理層部）である。

【０００３】次に、動作について説明する。図において、まず、コンソール端末から接続を許可するＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスの範囲を設定し、この設定内容をメモリ５１に保持する。次に、ハブ５０は、ＡＲＰ（Ａｄｄｒｅｓｓ　ＲｅｓｏｌｕｔｉｏｎＰｒｏｔｏｃｏｌ）フレームに含まれる送信元のＩＰアドレスを調べる。この送信元ＩＰアドレスが、メモリ５１に保持されている許可されたＩＰアドレスの範囲に含まれない場合は、不正な端末がネットワークに接続されていると判断し、適切なポート５３ｊをデータバス５２から切り離す。

【０００４】

【発明が解決しようとする課題】従来の侵入防止機能付きハブでは、不正なパケットか否かの判断を、パケットの送信元のＩＰアドレスを用いて、あらかじめ設定されている値か否かで判断していた。そのため、不正を行う侵入者が正式な要求元からアクセスする場合、不正な侵入であるにもかかわらず、不正なパケットであると判断できず、侵入されてしまう。

【０００５】また、侵入を防止するためにポートをきりはなした場合、正当な利用者からのパケット又は接続に対して自動的にポートをオープンする処置がされてない。そのため、再度ポートを使用可能とするためには、コンソールからの指示又は再起動といった管理者の操作が必要となる。端末等の装置が一つのフロアだけでなく、複数のフロア及び別建物にも配置されてある場合、侵入防止のために自動的に通信が遮断されることは、対策として有効であるが、いつまでも通信が遮断されていると、業務に必要な通信がいつまでたってもできず、業務に支障をきたす。攻撃に対処しつつ、円滑に業務システムを運用するためには、不正な侵入が行われてなければ、ただちに業務システムが再開されなくてはならない。

【０００６】この発明は、上記のような問題点を解決するためになされたもので、不正侵入の検知をパケットの要求元ではなくパケットから判断することを目的とする。また、不正なパケットである場合、不正侵入を防止する、通信の遮断等の対策をとることを目的とする。更に、不正侵入が行われてなければ、遮断されていた通信を管理者の手を煩わせることなく自動的に解除し、通信可能とすることを目的とする。

【０００７】

【課題を解決するための手段】この発明に係る侵入検知装置は、パケットを送受信する通信部と、上記通信部が受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析部と、上記パケット分析部が不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策部とを備えることを特徴とする。

【０００８】上記侵入検知装置は、さらに、上記パケット分析部の検出結果に基づいて上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視部と、上記不正侵入監視部が、不正侵入終了を判断した場合、上記対策部がとる上記不正侵入を防止する対策を解除する対策解除部とを備えることを特徴とする。

【０００９】上記パケット分析部は、予め定義するデータを含むパケットを不正なパケットであるとすることを特徴とする。

【００１０】上記パケット分析部は、予め定義するデータとして、通信プロトコルの名称と通信ポートの番号と所定の文字列との少なくともいずれか一つを定義することを特徴とする。

【００１１】上記対策部は、不正侵入を防止する対策として、不正なパケットの通信を遮断することを特徴とする。

【００１２】上記対策部は、通信の遮断として、使用していた通信ポートの使用を中止し、上記侵入検知装置は、さらに、上記対策部によって使用していた通信ポートの使用が中止されている場合、上記使用していた通信ポートとは別の通信ポートをオープンし、オープンした通信ポートを所定の送信元へ通知する通信ポート通知部を備えることを特徴とする。

【００１３】上記侵入検知装置は、さらに、不正なパケットの受信が終了した場合に、使用を中止した通信ポートの使用を再開し、上記通信ポートの再開を上記所定の送信元へ通知する不正侵入終了通知部を備えることを特徴とする。

【００１４】この発明に係る不正侵入対策管理システムは、情報処理装置と、上記情報処理装置と通信網を介して接続し、不正侵入を検知する侵入検知装置とを備える不正侵入対策管理システムにおいて、上記侵入検知装置は、上記通信網を介してパケットを送受信する通信部と、上記受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析部と、上記パケット分析部で不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策部と、上記対策部によって使用していた通信ポートの使用が中止されている場合、上記使用していた通信ポートとは別の通信ポートをオープンし、オープンした通信ポートを上記情報処理装置へ通知する通信ポート通知部とを備え、上記情報処理装置は、上記通信網へパケットを送信すると伴に、上記通信ポート通知部から通知される通信ポートを受信する送受信部と、上記送受信部によって受信した通信ポートを用いて通信することを設定するテンポラリポート設定部とを備えることを特

徴とする。

【００１５】上記侵入検知装置は、さらに、上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視部と、上記不正侵入監視部によって、不正侵入終了を判断した場合、上記不正侵入を防止する対策を解除する対策解除部と、不正なパケットの受信が終了した場合に、使用を中止した通信ポートの使用を再開し、上記使用を中止した通信ポートの再開を上記情報処理装置へ通知する不正侵入終了通知部とを備え、上記送受信部は、上記不正侵入終了通知部からの通知を受信し、上記テンポラリポート設定部は、上記使用を中止した通信ポートを用いる通信へ設定を変更することを特徴とする。

【００１６】この発明に係る侵入検知方法は、パケットを送受信する通信工程と、上記受信したパケットを分析し、分析したパケットの中から不正なパケットを検出するパケット分析工程と、上記パケット分析工程で不正なパケットを検出した場合に、不正なパケットが侵入する不正侵入を防止する対策をとる対策工程とを備えることを特徴とする。

【００１７】上記侵入検知方法は、さらに、上記不正侵入の有無を監視し、上記不正侵入が終了する不正侵入終了を判断する不正侵入監視工程と、上記不正侵入監視工程によって、不正侵入終了を判断した場合、上記不正侵入を防止する対策を解除する対策解除工程とを備えることを特徴とする。

【００１８】

【発明の実施の形態】実施の形態１．図１は、この発明の侵入検知装置及び侵入検知方法を示す実施例の構成図である。図１において、１００は受信したパケットに対して不正侵入が行われているか否かを分析し、侵入が行われていると判断した場合、通信遮断等の対策を行う侵入検知装置である。１１０はパケットを受信又は送信する通信手段（通信部）である。１２０は受信したパケットが不正であるか否かを判断するパケット分析手段（パケット分析部）である。１３０は通信遮断等の対策を行う対策手段（対策部）である。１４０は対策手段１３０によって対策が行われている場合、不正侵入が行われていないか否かを監視する不正侵入監視手段（不正侵入監視部）である。１５０は不正侵入監視手段１４０が不正侵入が行われていないと判断した場合、通信遮断等の対策を解除する対策解除手段（対策解除部）である。この明細書では、パケットは、ネットワーク上を流れる全てのデータを総称し、特定のデータを指しているわけではない。

【００１９】次に、動作について図２を用いて説明する。まず、侵入検知装置１００は、通信手段１１０により外部ネットワークからパケットを受信する（Ｓ１０）。そして、パケット分析手段１２０によりパケットが不正か否かを後述に示す例のように解析する（Ｓ２０）。もし、受信したパケットが不正であると判断した場合（Ｓ３０でＹｅｓ）、対策手段１３０によりパケットの中継は行わず、通信を遮断する（Ｓ４０）。そして、侵入検知装置１００は、不正侵入監視手段１４０を用いて、不正侵入が行われているか否かを後述に示す例のように監視する（Ｓ５０）。もし、不正侵入が行われていないと判断した場合（Ｓ６０でＹｅｓ）、対策解除手段１５０を用いて通信遮断を解除し（Ｓ７０）、パケットの中継を再開する（Ｓ８０）。

【００２０】以上のように、不正か否かの判断を、要求元のアドレスだけではなく、パケット内のデータ、コマンド、アクセスの頻度等によって判断しているので、侵入者が正規な要求元から侵入しようとしても侵入を検知することができる。

【００２１】また、不正侵入監視手段１４０と対策解除手段１５０を用いることにより、不正侵入が終了したら自動的に通信が再開しているため、管理者の手を煩わせることがなく管理者の作業が軽減する。

【００２２】次に、パケットの分析方法の例について説明する。パケットの分析方法には、大きくわけると次の２つの方法で行う。

（１）パケット内に含まれている文字列やコードを検査するパターンマッチング。

（２）一定時間に一定以上の個数のパケットを検知する統計的な手法。

【００２３】次に、上記（１）のパターンマッチングの例を３つ、上記（２）の統計的な手法の例を１つ示す。

パターンマッチング１：メールサーバへのバッファオーバーフロー攻撃の検知方法。

メールサーバへのバッファオーバーフロー攻撃を受けると、メールサーバは、異常終了、誤動作等正常に動作しなくなる。この攻撃を検知するためには、パケットが以下のようなパターンになっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ＝２５（ＳＭＴＰであることを表す）

ＴＣＰデータ

以下のｓｍｔｐコマンドの引数が１２８バイト以上か否かで判断。

“ｈｅｌｏ”，“ｍａｉｌ　ｆｒｏｍ：”，“ｒｃｐｔ　ｔｏ：”，“ｖｒｆｙ”，“ｅｘｐｎ”

メールサーバへのバッファオーバーフロー攻撃は、実際には、ｐｏｐ（Ｐｏｓｔ　Ｏｆｆｉｃｅ　Ｐｒｏｔｏｃｏｌ）に対してもあり、上記は、あくまでも一例である。また、メールサーバへの攻撃には、ｓｍｔｐ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）コマンドを利用してユーザ名・ユーザの有無などの情報取得といったさまざまな攻撃が存在する。

【００２４】パターンマッチング２：ＦＴＰ　ｃｗｄ　～ｒｏｏｔ攻撃の検知方法。

この攻撃を受けると、ｆｔｐ（Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）サーバは、ルート権限を取得される。そのため、パスワードファイル等の重要なファイルが改ざん又は盗まれたり、ウイルス等の不正処理を行うプログラムをセットアップされ、実行されて、ｆｔｐサーバが正常に動作しなくなる可能性がある。この攻撃を検知するためには、パケットが以下のようなパターンになっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ＝２１（ＦＴＰ－ＣＯＮＴＲＯＬ）ＴＣＰデータ

“ｃｗｄ　￣ｒｏｏｔ”の文字列を検知する。

“ｃｗｄ”は、ｆｔｐで使用される制御コマンドである。上記以外のコマンドを用いることも可能である。

【００２５】パターンマッチング３：ｈｔｔｐ　ｐｈｆのバグを用いた攻撃の検知方法。

この攻撃を受けると、ｈｔｔｐ（Ｈｙｐｅｒ　Ｔｅｘｔ　ＴｒａｎｓｆｅｒＰｒｏｔｏｃｏｌ）サーバは、ルート権限でコマンドを実行されてしまう。そのため、パスワードファイル等の重要なファイルが改ざん又は盗まれたり、ウイルス等の不正処理を行うプログラムをセットアップされ、実行されて、ｈｔｔｐサーバが正常に動作しなくなる可能性がある。この攻撃を検知するためには、パケットが以下のようなパターンになっているか否か分析する。

ＴＣＰヘッダ

Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ＝８０（ＨＴＴＰ）

ＴＣＰデータ

“ｇｅｔ”，“／ｐｈｆ”の文字列を検知する。

ｐｈｆは、プログラム名の１つである。上記以外のプログラム名を用いることも可能である。

【００２６】統計的な手法１：ＳＹＮフラッド攻撃の検知方法（サービス不能（ＤｏＳ）攻撃の一例）。

この攻撃をうけると、ＳＹＮパケット対応のためにリソースがなくなり、システムの負荷が高くなり、他のサービスを実行することができなくなる。この攻撃を検知するためには、一定時間内（例えば、１０秒間）に、以下に該当するパケットが一定個数（例えば、１００個）以上あるか否かを分析する。

ＩＰヘッダのＤｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓが共通。

ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ヘッダのＳＹＮフラグが１、ＡＣＫフラグが０。

ＳＹＮフラッド（ＳＹＮ－ｆｌｏｏｄ）は、攻撃名の１つである。上記以外の攻撃名を用いることも可能である。

【００２７】次に、侵入監視の例についてＤｏＳ攻撃の場合について説明する。ＤｏＳ攻撃に対する侵入が終了したか否かの判断は、一定時間内（例えば、１０秒間）に特定のパケットが一定個数（例えば、１００個）以下であるか否かで判断する。これらのしきい値は一例であり、攻撃の種類ごとに変更してもよい。また、攻撃と判断したときのしきい値と、攻撃終了と判断するときのしきい値とは同じでなくてもよい。

【００２８】なお、上記実施の形態１の例では、対策として、全パケットの通信を遮断した。そのため、全パケットの通信を遮断すると正常なパケットが通信されなくなる。そこで、攻撃の種類によってｉｃｍｐ，ｔｃｐ，ｕｄｐといったプロトコル毎にパケット中継を行わないようにすることによって、全パケットでなく攻撃に関するパケットだけを遮断してもよい。また、プロトコルごとではなく、ｔｃｐ又はｕｄｐ（Ｕｓｅｒ　Ｐａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）のポート番号毎に通信遮断することによって、正常なパケットは正常に通信できるように対策してもよい。すなわち、一例として、電子メールに関する攻撃があった場合、電子メールを表すｔｃｐポート番号２５のパケットだけを遮断することにより、Ｗｅｂサーバへのアクセス（ｔｃｐポート番号８０）や、ＦＴＰ（ｔｃｐポート番号２１）の通信が可能となる。また、送信元／先のアドレスごとに通信を遮断するように対策してもよい。また、ｔｃｐのセッションを確立して行う攻撃に対しては、ｒｅｓｅｔパケットを送信することによりｔｃｐセッションを切断してもよい。

【００２９】対策手段１３０が採り得る対策として、下記のような対策が想定される。

（Ａ）通信の遮断

（Ｂ）攻撃者に対して攻撃パケットを送信する（応戦、やり返す）

（Ｃ）うその応答を返す（おとり、相手に侵入成功と思わせる）

上記は一例であり、上記以外の対策方法であってもかまわない。

【００３０】通信の遮断は、侵入検知装置１００へ転送されたパケットを破棄することによって実施する。通信を遮断する際には、侵入検知装置１００へ転送されたパケット全てを破棄してもよいし、一部を破棄してもよい。通信の遮断には、ポートのクローズ、プロトコルのクローズも含まれる。ポートのクローズは、通信ポートが同一のパケットを破棄することによって実施する。また、プロトコルのクローズは、通信プロトコルが同一のパケットを破棄することによって実施する。

【００３１】また、この実施の形態では、パケット分析手段１２０によって、不正侵入が検出された後も、送信元から侵入検知装置１００へパケットは転送される。侵入検知装置１００へ転送されるパケットは、パケット分析手段１２０によって全てのパケットが分析され、分析結果に基づいて、不正侵入監視手段１４０は、不正侵入が終了したか否かを監視する。

【００３２】さらに、上記のように、不正侵入検出後、パケット分析手段１２０は、侵入検知装置１００に転送される全てのパケットを分析しているが、不正を検出したパケットと同一のパケットを検査する手段を別に備えるようにしてもよい。すなわち、不正侵入検出後、検出した不正だけを検査する分析プログラムのように機能をわけることも可能である。具体的には、すべての項目を分析するプログラムと、特定の項目だけを分析するプログラムとに分けることも可能である。

【００３３】また、パターンマッチングに用いるデータとして、制御コマンド、プログラム名、攻撃名を用いる場合を示したが、これらに限られることはない。上記以外のデータを用いてもよい。

【００３４】以上のように、コンピュータネットワークシステムにおいて、以下の手段を備えた侵入検知装置及び以下の手段を備えた侵入検知装置を用いた不正侵入対策管理システムであることを特徴とする。

（ａ）通信手段、（ｂ）受信したパケットを解析して不正侵入が行われているか否かを判断するパケット分析手段、（ｃ）不正侵入が行われていると判断した場合、プロトコル又はポートのクローズ、通信遮断等を行う対策手段。

【００３５】更に、上記侵入検知装置は、以下の手段を備える。

（ｄ）不正侵入等の攻撃が終了したか否かを監視する不正侵入監視手段、（ｅ）不正侵入等の攻撃が終了したと判断した場合、通信遮断等の対策を解除する対策解除手段。

【００３６】実施の形態２．以上の実施の形態では、侵入検知装置１００には、パケット分析手段１２０、対策手段１３０及び対策解除手段１５０が、同じ装置上に装備される例である。しかし、それぞれの手段は、同じ装置上に実装しなくてもよい。例えば、次のように構成することもできる。侵入検知装置１００の他に、対策を実施する対策装置と、それら対策装置を管理する管理装置を設ける。侵入検知装置１００は、攻撃が行われているか終了しているかを管理装置に通知する。管理装置は、通知の内容にしたがって対策装置に対策の指示又は対策の解除指示を行ってもよい。

【００３７】実施の形態３．以上の実施の形態１では、不正侵入されている場合の対策として、通信を遮断したものである。しかし、その場合、同一プロトコル又は同一ポートを利用した正常なパケットの通信も遮断されてしまう。そこで、次に、正常なパケットを通過させるために、テンポラリのポートを利用して正常なパケットを通信する場合の実施の形態を示す。

【００３８】図３は、このような場合の不正侵入対策管理システムを示す実施例の構成図である。図３において、Ｂは受信したパケットが不正か否かを分析する侵入検知装置である。３０ｊ（ｊ＝１～Ｎ）は業務等の情報処理を行う情報処理装置３０ｊである。

【００３９】図４は、侵入検知装置２００の構成図の一例である。図４において、２１０はパケットを受信又は送信する通信手段（通信部）である。２２０は受信したパケットが不正であるか否かを判断するパケット分析手段（パケット分析部）である。２３０は通信遮断等の対策を行う対策手段（対策部）である。２３１はテンポラリの通信路を通知する通信ポート通知手段（通信ポート通知部）である。２４０はパケット分析手段２２０によって検知した攻撃がまだ行われているか否かを監視する不正侵入監視手段（不正侵入監視部）である。２５０は不正侵入監視手段２４０が不正侵入が行われていないと判断した場合、通信遮断等の対策を解除する対策解除手段（対策解除部）である。２５１は、不正侵入監視手段２４０が不正侵入が行われてていないと判断した場合、情報処理装置３０ｊ（ｊ＝１，・・・，Ｎ）に不正侵入が終了しことを通知する不正侵入終了通知手段（不正侵入終了通知部）である。

【００４０】図５は、情報処理装置３０ｊ（ｊ＝１，・・・，Ｎ）の構成図の一例である。図５において、３１０は送受信手段（送受信部）、３２０は侵入検知装置２００から指定された通信路で通信することを設定するためのテンポラリポート設定手段（テンポラリポート設定部）である。

【００４１】次に、動作を図６を用いて説明する。図２と同じステップ番号の処理は、同様な処理を示す。侵入検知装置２００は、通信手段２１０によって受信したパケット（Ｓ１０）をパケット分析手段２２０を用いて分析する（Ｓ２０）。分析の結果、パケットが不正であると判断した場合（３０でＹｅｓ）、対策手段２３０によりパケットの中継は行わず通信を遮断する（Ｓ４０）。また、通信ポート通知手段２３１は、不正パケットが使用していたポート番号（例えば、２５）とは異なり、他のアプリケーションで使用していない番号（例えば、９０００）を選択し（Ｓ４１）、通信ポート通知手段２３１を用いて情報処理装置３０ｊに２５番を使用していたアプリケーションに９０００で通信するよう通知する（Ｓ４２）。

【００４２】情報処理装置３０ｊは、変更する通信ポート番号を受信し（Ｓ１００）、テンポラリポート処理手段３２０を用いて、通信ポートの設定を変えることによって、２５番を使用していたアプリケーションは９００００番を用いて通信を実施する（Ｓ１０１）。

【００４３】侵入検知装置２００は、不正侵入監視手段２４０によって実施の形態１と同様に、不正侵入が行われているか否かを監視する（Ｓ５０）。そして、侵入検知装置２００は、不正侵入監視手段２４０によって攻撃が終了したと判断した場合（Ｓ６０でＹｅｓ）、対策解除手段２５０を用いて通信遮断を解除し（Ｓ７０）、パケットの中継を再開する（Ｓ８０）。また、不正侵入終

了通知手段２５１を用いて情報処理装置３０ｊに攻撃が終了したことを通知することにより（Ｓ７１）、情報処理装置３０ｊは、通常のポート番号２５で通信を再開する（Ｓ１１０，Ｓ１１１）。

【００４４】以上のように、対策のためにあるポートを閉じたとしてもテンポラリのポートを利用しているため、閉じられたポートで通信していた正常なパケットは通信が遮断されずに送受信可能となり、システムは停止せず業務等のアプリケーションは稼動しつづけることができる。

【００４５】なお、上述の例では、テンポラリのポート選択及び通知を侵入検知装置２００で行ったが、必ずしも侵入検知装置２００で行う必要はない。侵入検知装置２００の他に、各アプリケーションが利用しているポートの管理等を行う管理装置を設け、侵入検知装置２００は、管理装置に閉じたポートを通知し、管理装置がテンポラリのポートを選択及び各アプリケーションへ通知してもよい。また、図４では、通信ポート通知手段２３１は、対策手段２３０に含まれる構成を示したが、通信ポート通知手段２３１は、対策手段２３０とは別個の構成要素であってもよい。同様に、不正侵入終了通知手段２５１は、対策解除手段２５０と別個の構成要素であってもよい。

【００４６】以上のように、コンピュータネットワークシステムにおいて、実施の形態１の侵入検知装置に加え、以下の手段を備えた侵入検知装置及び上記侵入検知装置を用いた不正侵入対策システムであることを特徴とする。

（ｆ）プロトコル又はポートのクローズといった通信遮断がされている場合、テンポラリにポートをオープンする手段、（ｇ）テンポラリにオープンしたポートを通知する手段。

【００４７】更に、上記不正侵入対策システムは、以下の手段を備えた情報処理装置を備える。

（ａ）侵入検知装置からのテンポラリにオープンしたポートの通知を受信する手段、（ｂ）テンポラリにオープンされたポートを利用して通信を行う手段、（ｃ）侵入検知装置からの攻撃終了の通知を受信し、本来のポートで通信を再開する手段。

【００４８】

【発明の効果】以上のように、この発明は、パケットの内容で不正か否かを判断することにより、正規な要求元からの攻撃を検知できるという効果がある。

【００４９】また、対策実施後（例えば、ポートを閉じた後）、攻撃が続行しているか否かを監視し、攻撃が終了していた場合、対策解除（例えば、ポートオープン）することにより、人手を介さずに自動的に対策を解除できるため、対策終了後迅速に業務・サービスの提供が再開できる。そして、自動的に対策が解除されるため、対策解除のための管理者の作業を省くことができ、コンピュータネットワークシステムの管理運用に関する人的作業を軽減できる。

【００５０】この発明によれば、所定のデータに基づいて、不正パケットを検出することができる。

【００５１】この発明によれば、通信を遮断することによって、不正なパケットが転送されることを防止することができる。

【００５２】また、攻撃の対策として、通常使用するポートを閉じてしまっても、各アプリケーション（情報処理装置）にテンポラリのポートを通知し、各アプリケーションはテンポラリのポートで通信を行うため正常な利用者にはアプリケーションのサービスを提供することができる。

【００５３】この発明によれば、対策終了後、使用を中断していた通信ポートを迅速に、自動的に再開することができる。

【図面の簡単な説明】

【図１】　実施の形態１の侵入検知装置の一例を示す構成図。

【図２】　実施の形態１の侵入検知方法の動作の一例を表すフローチャート図。

【図３】　実施の形態２の不正侵入対策管理システムの全体構成の一例を示す図。

【図４】　実施の形態２の侵入検知装置の一例を示す構成図。

【図５】　実施の形態２の情報処理装置の一例を示す構成図。

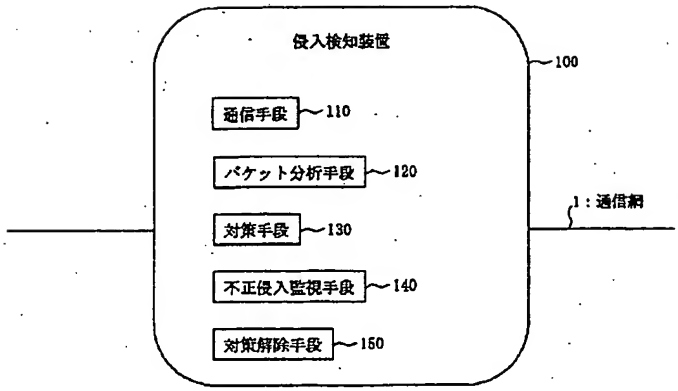
【図６】　実施の形態２の侵入検知方法の動作の一例を表すフローチャート図。

【図７】　従来例の実施例を示す構成図。

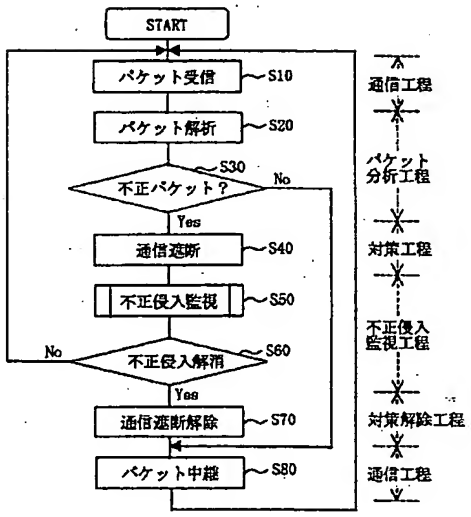
【符号の説明】

１　通信網、５０　ハブ、５１　メモリ、５２　データバス、５３ｊ（ｊ＝１～Ｎ）　ポート、１００，２００　侵入検知装置、１１０，２１０　通信手段、１２０，２２０　パケット分析手段、１３０，２３０　対策手段、１４０，２４０　不正侵入監視手段、１５０，２５０　対策解除手段、２３１　通信ポート通知手段、２５１　不正侵入終了通知手段、３０１～３０Ｎ，３０ｊ（ｊ＝１～Ｎ）　情報処理装置、３１０　送受信手段、３２０　テンポラリポート設定手段。

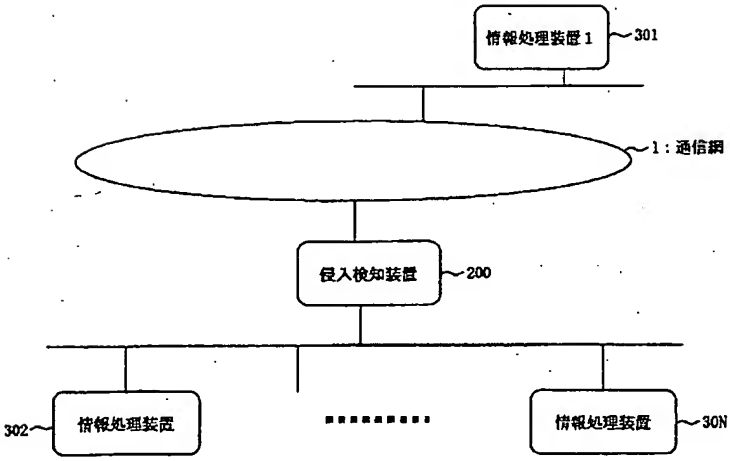
【図1】


侵入検知装置
100
通信手段
110
パケット分析手段
120
対策手段
130
不正侵入監視手段
140
対策解除手段
150
1：通信網

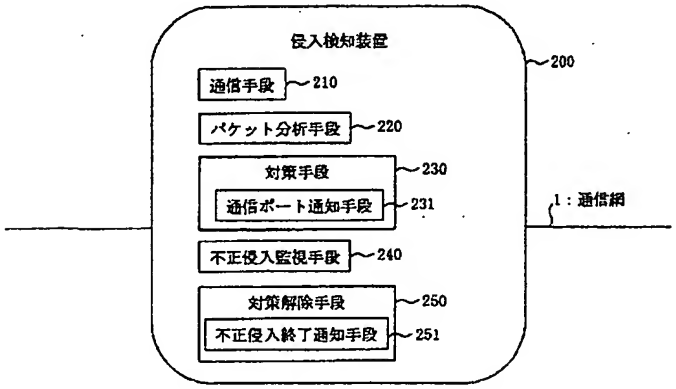
【図2】


START
パケット受信
S10
パケット解析
S20
S30
不正パケット？
No
Yes
通信遮断
S40
不正侵入監視
S50
No
不正侵入解消
S60
Yes
通信遮断解除
S70
パケット中継
S80
通信工程
パケット分析工程
対策工程
不正侵入監視工程
対策解除工程
通信工程

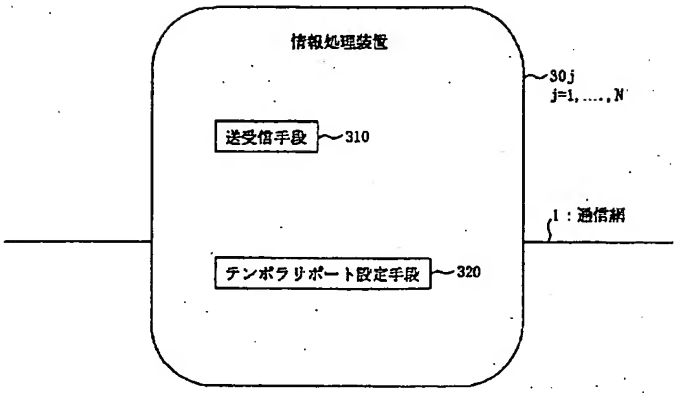
【図3】


情報処理装置1
301
1：通信網
侵入検知装置
200
302
情報処理装置
情報処理装置
30N

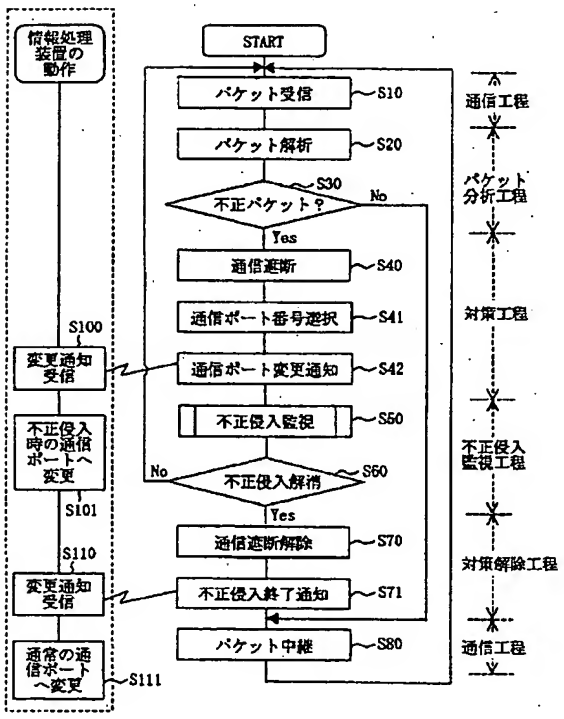
【図4】


侵入検知装置
200
通信手段
210
パケット分析手段
220
対策手段
230
通信ポート通知手段
231
不正侵入監視手段
240
対策解除手段
250
不正侵入終了通知手段
251
1：通信網

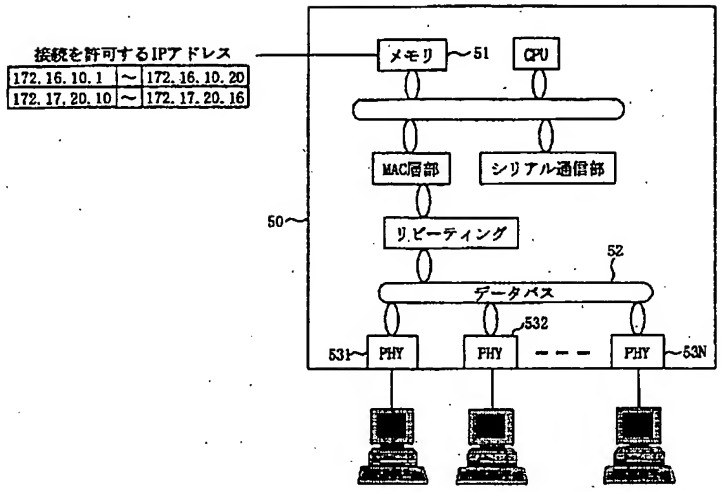
【図5】


情報処理装置
30j
j=1,....,N
送受信手段
310
1：通信網
テンポラリポート設定手段
320

【図6】


情報処理装置の動作
START
パケット受信
S10
パケット解析
S20
S30
不正パケット？
No
Yes
通信遮断
S40
通信ポート番号選択
S41
通信ポート変更通知
S42
不正侵入監視
S50
No
不正侵入解消
S60
Yes
通信遮断解除
S70
不正侵入終了通知
S71
パケット中継
S80
S100
変更通知受信
不正侵入時の通信ポートへ変更
S101
S110
変更通知受信
通常の通信ポートへ変更
S111
通信工程
パケット分析工程
対策工程
不正侵入監視工程
対策解除工程
通信工程

【図7】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	ﾃｰﾏｺｰﾄﾞ(参考)
H04L 12/22			